(19)日本国特許庁（ＪＰ）　(12)公表特許公報（Ａ）　(11)特許出願公表番号
特表2002－524808
（P2002－524808A）
(43)公表日　平成14年８月６日(2002.8.6)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ｂ	５Ｂ０１７
Ｇ０６Ｋ　19/073		Ｇ０９Ｃ　1/00	６４０Ｚ	５Ｂ０３５
Ｇ０９Ｃ　1/00	６４０	Ｇ０６Ｋ　19/00	Ｐ	５Ｊ１０４
Ｈ０４Ｌ　9/10		Ｈ０４Ｌ　9/00	６２１Ａ	

審査請求　未請求　予備審査請求　有　（全 24 頁）

(21)出願番号　特願2000－569595(P2000－569595)
(86)(22)出願日　平成11年９月１日(1999.9.1)
(85)翻訳文提出日　平成13年３月２日(2001.3.2)
(86)国際出願番号　ＰＣＴ／ＦＩ９９／００７１３
(87)国際公開番号　ＷＯ００／１４９８４
(87)国際公開日　平成12年３月16日(2000.3.16)
(31)優先権主張番号　９８１９０２
(32)優先日　平成10年９月４日(1998.9.4)
(33)優先権主張国　フィンランド（ＦＩ）

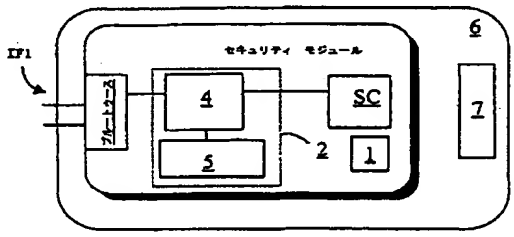
(71)出願人　ソネラ　スマートトラスト　オサケユキチュア
フィンランド国，エフアイエヌ－00510　ヘルシンキ，テオリスウスカツ　15
(72)発明者　パタネン　ハリ
フィンランド国，エフアイエヌ－00660　ヘルシンキ，レポランティエ　25　エー　3
(74)代理人　弁理士　八田　幹雄　（外４名）

Ｆターム(参考)　5B017 AA03 BA07 CA14
5B035 AA13 BB09 BC00 CA11
5J104 AA09 NA35 NA41 PA02 PA10

最終頁に続く

(54)【発明の名称】　セキュリティモジュール、セキュリティシステム、および移動局

(57)【要約】
本発明は、高度のデータ機密保護を与えるサービスおよび装置の実現に関する。特に、本発明は、セキュリティモジュール、セキュリティシステムおよびこれらに使用される移動局に関する。本発明は、バンキングサービスおよび他の高度なデータ機密保護を必要とするサービスを実現するために、容易に、かつ、何の改良もなく標準的な装置を使用することを可能とする。本発明では、伝送されるメッセージの伝送のための標準化されたローカルインターフェースを使用するように、セキュリティモジュールが形成されている。電気通信網によって生じるいかなる遅延もなくリアルタイムにメッセージが伝送される。



【特許請求の範囲】

【請求項１】　移動局、レジ端末、オンラインバンキング端末、あるいはそれらの同等物のような端末装置（ＳＰ）にセキュリティモジュールを接続するための接続手段（１）を有する前記セキュリティモジュールであって、

前記セキュリティモジュールを通してなされる電子データ転送を暗号化し、暗号化された情報を解読し、電子署名を実現するための暗号化手段（２）と、

電子データ転送を可能にするために外部デバイスに前記セキュリティモジュールを接続するための第１接続インターフェース（ＩＦ１）と、

電力を必要とする前記セキュリティモジュールの構成要素に電力を供給するための電源（３）と、

を有することを特徴とするセキュリティモジュール。

【請求項２】　前記暗号化手段は、

暗号化し、解読し、および電子署名を実現するプロセッサ（４）と、

前記プロセッサに必要とされるキーおよびパラメータを保管するために前記プロセッサに接続されるメモリ（５）と、

を有することを特徴とする請求項１に記載のセキュリティモジュール。

【請求項３】　前記セキュリティモジュールは、

前記セキュリティモジュールを通してスマートカード機能を実現するために設けられたスマートカード構成要素（ＳＣ）を有することを特徴とする請求項１または請求項２に記載のセキュリティモジュール。

【請求項４】　前記第１接続インターフェースは、ブルートゥースの技術使用して実現されることを特徴とする請求項１から請求項３のいずれか一項に記載のセキュリティモジュール。

【請求項５】　前記セキュリティモジュールは、

移動局の電源の形状に一致するために適したフレームと、

実質的に前記移動局の電源の代わりに前記セキュリティモジュールを接続するため、および前記電源（３）から前記移動局に電力を供給するために、前記フレームに取り付けられるコネクタ（７）と、

を有することを特徴とする請求項１から請求項４のいずれか一項に記載のセキ

ュリティモジュール。

【請求項６】　予め選択された通信リンクを通して電気的に相互に接続されるサービスプロバイダの端末（ＳＰ）と、サービス利用者の端末（ＭＳ）とを有するセキュリティシステムであって、

前記サービスプロバイダの端末に接続された第１セキュリティモジュール（ＳＭ１）と、

前記サービス利用者の端末に接続された第２セキュリティモジュール（ＳＭ２）とを有し、

前記各セキュリティモジュールは、端末間で通信リンクを通して伝送された情報を処理するために設けられ、

前記第１および第２セキュリティモジュールは、好ましくは、

前記セキュリティモジュールを通してなされた電子データ転送を暗号化し、暗号化された情報を解読し、電子署名を実現するための暗号化手段（２）と、

電子データ転送のために端末に前記セキュリティモジュールを接続するための第１インターフェース（ＩＦ１）と、

電力を必要とするセキュリティモジュールの構成要素に電力を供給するための電源（３）とを有することを特徴とするセキュリティシステム。

【請求項７】　前記サービスプロバイダの端末（ＳＰ１）は、オンラインバンキング端末、レジ、自動販売機、あるいはそれらの同等物であることを特徴とする請求項６に記載のセキュリティシステム。

【請求項８】　サービス利用者の端末（ＳＰ２）は、移動局、ポータブルコンピュータ、あるいはそれらの同等物であることを特徴とする請求項６または請求項７に記載のセキュリティシステム。

【請求項９】　サービスプロバイダのサーバ（８）を有し、

前記第１セキュリティモジュールは、サービス利用者の端末によって実行される機能を更新し、更新した前記機能を前記サーバに保管するために前記サービスプロバイダのサーバ（８）に前記電気通信網を通して接続されていることを特徴とする請求項６から請求項８のいずれか一項に記載のセキュリティシステム。

【請求項１０】　キーパッド（９）と、ディスプレイ（１０）と、無線装置

（１１）と、電源（１２）とを有する移動局であって、

前記セキュリティモジュールを通してなされる電子データ転送を暗号化し、暗号化された情報を解読し、電子署名を実現するための暗号化手段（２）と、電子データ転送を可能とするために、前記移動局（ＭＳ）および／または外部デバイス（ＳＰ）に前記セキュリティモジュールを接続するための第１インターフェース（ＩＦ１）とを有し、前記電源と統合されるセキュリティモジュール（ＳＭ）

を有することを特徴とする移動局。

【請求項１１】　前記セキュリティモジュール（ＳＭ）は、電気通信網および／または移動局のローカルインターフェース（１３）を通して移動局によって伝送される情報を処理するために設けられたことを特徴とする請求項１０に記載の移動局。

【請求項１２】　セキュリティモジュール（ＳＭ）は、ブルートゥースの技術を使用することによって、移動局（ＭＳ）および／またはサービスプロバイダの端末（ＳＰ）と通信するために設けられていることを特徴とする請求項１０または請求項１１に記載に移動局。

【発明の詳細な説明】

【０００１】

発明の技術分野

本発明は、セキュリティモジュールに関する。特に、本発明は、高度なデータ機密保護を必要としているさまざまなメッセージを処理および伝送するための新しく、そして改良されたセキュリティモジュール、および、セキュリティシステムに関する。本発明は、また、セキュリティモジュールを利用している移動局に関する。

【０００２】

発明の背景

たとえば、ＧＳＭネットワーク(GSM, Global System for Mobile communications)などの移動体通信ネットワークでは、移動局および基地局間における無線リンクによる音声の伝送と連動して、大量の暗号化が使用される。また、音声通信の他に、テキストあるいはデータメッセージを使用する通信が増加している。サービス水準の向上とともに、テキストあるいはデータ通信に依存しているサービスが普及してきている。テキスト通信は、代金支払いのためのサービスなどにおいて、さまざまなサービス機能に利用できる。

【０００３】

現在、メッセージを暗号化することに問題となる原因は、事実、移動体通信に関して現在の標準と整合した携帯電話では、電話に使用されるユーザインターフェースがメーカ特有であるため、暗号化を促進するためのいかなる変更も可能でない。暗号化に関して、十分に標準化され、十分に開かれている唯一の構成要素は、加入者識別モジュール（ＳＩＭ）である。

【０００４】

ＧＳＭ標準規格のような現在の移動体通信の標準規格と整合した携帯電話は、移動局を通してテキスト通信を暗号化する可能性を直接的には供給しない。テキスト通信は、銀行サービスのような高度なデータ機密保護が要求されるサービスの実行に使用されることができる。しかしながら、高度なデータ機密保護が要求されるサービスは、メッセージ通信の十分な暗号化が可能になる前には普及する

ことができない。

【０００５】

移動体通信ネットワークを使用する更なる問題は、その移動体通信ネットワークにおいて実現されるメッセージ伝送サービスが必ずしもリアルタイムのサービスであるというわけではなく、メッセージの伝送に時間がかかるということである。これは、たとえば、ユーザが店のレジで買い物の代金を払いたいときに問題となる。この場面では、メッセージ伝送のわずかな遅延さえ、支払い処理の実行を著しく妨害する。現在、移動体通信の標準規格の一部分も、移動局およびレジ端末間のローカル通信をサポートしていない。

【０００６】

電気通信および情報技術において世界的にその業界を導く一団が、携帯電話と、たとえばポータブルコンピュータとの無線接続の確立を可能とする技術を発達させた。この技術は、「ブルートゥース（Ｂｌｕｅｔｏｏｔｈ）」と呼ばれ、短距離無線技術に基づき、多くのタイプの端末を相互に接続させるために使用することができる。この技術は、たとえば、WWWページのwww.bluetooth.comにおいてより詳細な説明されている。

【０００７】

ブルートゥースの技術は、短距離無線リンクを通して、複数の装置を相互に接続することを可能にする。ブルートゥースの技術を使用することによって、たとえば、移動局およびポータブルコンピュータ間で、厄介なケーブルをなくして接続を確立することが可能である。プリンタ、ワークステーション、電話ファックス装置、キーボード、および、ほとんどいかなるデジタル装置も、ブルートゥースシステムあるいはネットワークの部分となることができる。その技術は、既存のデータネットワークおよび周辺装置に万能のブリッジを形成し、固定されたネットワークインフラストラクチャを用いずに相互に接続された装置を通して、小さい個人的なグループを形成するための手段を提供する。加えて、たとえば、一定のポータブルコンピュータとの接続には、一定のユーザの携帯電話のみが使用されることが出来るように、暗号化および認証を、装置間の通信に使用することができる。

【０００８】

スマートカードもまた以前から知られており、それは、確実な個人の認証および真正の署名を可能にする。その適用の範囲は、無制限である。適用可能な実例としては、国民の電子識別カード（ＥＩＤ）、ファイルの暗号化、電気通信および電子メール、証書に署名するための手段、電子通貨、運転免許証、投票などがある。

【０００９】

スマートカードが上記した方法に使用できるとはいえ、スマートカードは当該スマートカードと通信するための別の読取装置をさらに必要とするという問題が残る。さらに、スマートカードだけでは電気通信網を介して通信することができず、それは、たとえばショートメッセージを使用している情報を更新することが不可能であることを意味する。

【００１０】

加えて、ブルートゥースの技術を使用して移動局をローカルにレジ端末に接続可能で、かつ、支払い装置として移動局が利用可能であるとしても、支払い処理のために必要とされるデータ通信を暗号化して、守るという問題がさらに残る。

【００１１】

従来技術では、異なるレジおよび自動化システム、移動局あるいは他のポータブル装置に接続されることができ、銀行および権限によって課された高いデータ機密保護の要求を満たすように、たとえばブルートゥースの技術を利用して、たとえば一方でホスト装置に、他方でサービスプロバイダの装置と安全に通信できる汎用セキュリティモジュールは知られていない。

【００１２】

本発明の目的は、上述される問題を解消することである。

【００１３】

本発明の特定の目的は、暗号化されて安全なローカル接続のための多くの種類の適用環境に使用されることができる新型の汎用セキュリティモジュールを開示することである。本発明の更なる目的は、ユーザおよびサービスプロバイダ間でデータ通信を暗号化するための手段を提供するセキュリティシステムを開示する

ことである。

【００１４】

本発明の更なる目的は、高度のデータ機密保護で、サービスプロバイダの端末とのローカル通信のために使用されることができる新型の移動局を開示することである。セキュリティモジュールと共にこのソリューションを使用することによって、いかなる環境にでも接続され、使用されることができる汎用セキュリティ装置を実現することが可能である。

【００１５】

付加的な本発明の目的は、装置メーカがいわゆる信頼できる第三者として直接保証されることができる装置を開示することである。これは、たとえば携帯電話メーカのような一定のメーカにより製作される装置に対して、信頼できる第三者によって個々に暗号化プロパティを加える必要性を除去する。

【００１６】

発明の簡単な説明

本発明は、たとえば、移動局、レジ端末、オンラインバンキング端末、ポータブルコンピュータ、電話、あるいは他の対応する端末に、セキュリティモジュールを接続するための接続手段を有するセキュリティモジュールに関する。そのセキュリティモジュールは、電気通信網および電気通信端末に接続される汎用モジュールを意図し、高度のデータ機密保護を必要とするアプリケーションの実行のために必要とされる暗号化操作を実現可能にする。

【００１７】

本発明によれば、そのセキュリティモジュールは、当該セキュリティモジュールを介してもたらされる電子データ転送を暗号化し、暗号化された情報を解読し、電子署名を実行するための暗号化手段を有する。暗号化手段は、好ましくは、暗号化し、解読し、電子署名を実行するためのプロセッサを有する。加えて、上記手段は、必要なキーおよびパラメータを記憶するためにプロセッサに接続されるメモリを有する。

【００１８】

さらに、本発明によれば、セキュリティモジュールは、当該セキュリティモジ

ュールを電子データ転送のための外部デバイスに接続するための第１接続インターフェースと、電力を消費しているにセキュリティモジュールの構成要素（すなわちプロセッサおよびメモリ）に電力を供給するための電源とを有する。電源は、また、ホスト装置から直接セキュリティモジュールに電力を供給することによって、セキュリティモジュールが接続されるホスト装置の電源に置き換えられてもよい。その接続インターフェースは、たとえばブルートゥースの技術を使用して実行されることができる。なお、ブルートゥースの技術は、それ自体知られている技術であり、その標準化はまだ完了されていない。とにかく、それについては、以前から知られているので、ここでは説明しない。

【００１９】

加えて、セキュリティモジュールは、セキュリティモジュールとともにスマートカード機能を実行するために用意されたスマートカード装置を有してもよい。そのスマートカード装置は、たとえば、レジ端末、オンラインバンキング端末、および、電子マネーを使用およびダウンロードするためのそれらの同等物のような外部デバイスと通信するための接続インターフェースを使用できる。したがって、本発明は、クライアントおよびユーザにとって、スマートカードの使用をより簡単で、より魅力的なものにする。

【００２０】

セキュリティモジュールは、たとえば、移動局の電源と統合されることができ、この場合、セキュリティモジュールは、たとえば、移動局の電源の形状に一致するために適したフレームと、そのフレームに取り付けられ、移動局の電源の代わりに移動局に電気的にセキュリティモジュールを接続するために使用されるコネクタとを有することが好ましい。この場合、セキュリティモジュールは、移動局に電力を供給するため、および移動局によって通信を実行するために当該移動局に接続される。セキュリティモジュールは、直ちに、移動局のキーパッドを使用して操作されることができる。

【００２１】

本発明は、また、オンラインバンキング端末、レジ、自動販売機、またはそれらの同等物のようなサービスプロバイダの端末と、移動局のようなサービス利用

者の端末とを含むセキュリティシステムに関する。そのシステムでは、端末は、たとえば、ブルートゥースの技術を使用する予め選択された通信リンクを通して、電気的に相互に接続される。

【００２２】

本発明によれば、セキュリティシステムは、サービスプロバイダの端末に接続される第１セキュリティモジュールと、サービス利用者の端末に接続される第２セキュリティモジュールとを有する。それらのセキュリティモジュールによって、端末間の通信は、暗号化され、解読される。セキュリティモジュールは、暗号化手段と、第１インターフェースと、電源とを上述のようにセキュリティモジュールと連動して有することが好ましい。

【００２３】

セキュリティシステムは、また、サービスプロバイダの端末に電気的に接続されたサービスプロバイダのサーバを有してもよい。この接続は、たとえば、ＧＳＭネットワークあるいは他の適切なネットワークのような電気通信網を通して確立されることができる。第１セキュリティモジュールは、サービス利用者の端末を通して複数の機能を更新し、それらをサーバに保管するために、電気通信網を介してサービスプロバイダの端末にさらに接続されることができる。これは、サービスプロバイダの勘定に対して、サービスまたは買い物のためにサービス利用者によって支払われる電子マネーを転送するために使用される、いわゆる、クリアリング機能に関連する。

【００２４】

本発明は、また、キーパッド、ディスプレイ、無線装置、および電源を有する移動局（ここでは、それ自体公知の端末を意味する）に関する。この種類の移動局の好適な実例は、ＧＳＭ(GSM, Global Standard for Mobile Communication)互換端末あるいはＧＳＭ携帯電話である。

【００２５】

本発明によれば、移動局は、電源と統合され、暗号化手段を含むセキュリティモジュールと、第１接続インターフェースとを、上述のようにセキュリティモジュールと連動して有する。セキュリティモジュールは、電気通信網を超えて、お

よび／または移動局のローカル通信インターフェースを介して、移動局によって伝送された情報を処理するために設けられることが好ましい。セキュリティモジュールは、ブルートゥースの技術を使用することによって、移動局および／または外部の端末と通信してもよい。

【００２６】

本発明は、現在使用されている既存の携帯電話を安全な通信で使用するためにいかなる変更も必要でない点で、従来技術より優れている。本発明のさらに優れた点は、セキュリティモジュールが、暗号化されたデータ転送が必要であるほとんどすべての端末に接続可能である汎用装置であることである。

【００２７】

加えて、本発明は、たとえばオンラインバンキングサービスのような高度のデータ機密保護を必要とするサービスを提供するために、サービスプロバイダによって使用可能な安全なシステムの実現を可能とする。

【００２８】

以下では、添付図面を参照して、実施の形態の好適な実例によって本発明を説明する。

【００２９】

発明の詳細な説明

図１に示されるセキュリティモジュールは、端末ＳＰ、ＭＳにセキュリティモジュールを接続するための接続手段１を含む。端末は、移動局、レジ端末、オンラインバンキング端末、または高度のデータ機密保護を必要とするアプリケーションの実行に使用されるあらゆる該当装置である。さらに、セキュリティモジュールは、必要とされるときに、セキュリティモジュールにおける電子データ転送を暗号化、暗号化された情報を解読、および電子署名を生成するための暗号化手段２を含む。

【００３０】

ローカルネットワークインターフェースあるいはその同等物を実現するために、セキュリティモジュールは、たとえば、電子データ転送のための無線リンクを通してセキュリティモジュールが端末に接続されることを可能にする第１接続イ

ンターフェースＩＦ１をさらに含む。本発明の技術によって要求される動作を実行するために、図１に示すように、接続インターフェースと連動して、いわゆるブルートゥース構成要素を提供することが可能である。セキュリティモジュールは、また、電力を必要とするセキュリティモジュール構成要素に電力を供給するために、たとえば、充電可能な蓄電池、コンセントを使うトランス、あるいはそれらの同等物などのような電源３が提供される。

【００３１】

図１に示される暗号化手段は、暗号化機能のために特別に設計および活用され、暗号化、解読および電子署名を実行するためのプロセッサ４と、プロセッサに必要とされるキーおよびパラメータの記憶のためにプロセッサに接続されるメモリ５とをさらに含む。個人キーセキュリティモジュールの利用者、使用される暗号化アルゴリズムのパラメータ、および他の必要なデータは、メモリに記憶することが可能である。暗号化アルゴリズムの好適な実例はＲＳＡ方式であるが、アプリケーションにしたがって、他の非対称的なアルゴリズムが使用されてもよい。

【００３２】

さらに、セキュリティモジュールは、セキュリティモジュールによって、スマートカード機能を実行するためのスマートカード構成要素ＳＣを含む。スマートカード構成要素は、たとえば、電気通信接続のためのインターフェースＩＦ１のような、セキュリティモジュールの他構成要素を利用できる。

【００３３】

セキュリティモジュールのプロセッサ４あるいはスマートカード構成要素ＳＣは、セキュリティモジュールの機能を同期および計時するためのクロックをさらに含む。そのクロックは、セキュリティモジュールが接続される装置のクロックと同期される。また、そのクロックは、ブルートゥースシステムのクロックに同期される可能性もある。

【００３４】

セキュリティモジュールのフレーム６は、移動局の電源の形状に一致するように合わされる。加えて、フレーム６は移動局にセキュリティモジュールを接続す

るためのコネクタ７については提供される。セキュリティモジュールおよび移動局間の電力およびデータ通信は、コネクタ７を通して接続されることができる。本実施の形態において、セキュリティモジュールの電源は、実質的に、容量の点では移動局の電源に一致するので、充電も可能である。セキュリティモジュールは、機械的に、および電気的に簡単に移動局に接続することができる。

【００３５】

図２は、発明のセキュリティシステムの実例を示す。図２に示されるセキュリティシステムは、本実施の形態ではオンラインバンキング端末であるサービスプロバイダの端末ＳＰと、本実施の形態ではＧＳＭ携帯電話であるサービス利用者の端末ＭＳとを含む。ここで、サービスプロバイダの端末ＳＰとサービス利用者の端末ＭＳとは、予め選択された通信リンクを介して互いに電気的に接続されている。本実施の形態では、通信リンクは、ブルートゥースの技術を使用して確立される。

【００３６】

図２に示されるセキュリティシステムは、加えて、サービスプロバイダの端末に接続された第１セキュリティモジュールＳＭ１と、サービス利用者の端末に接続されたセキュリティモジュールＳＭ２とを含み、これらのセキュリティモジュールは、電気通信リンクを通して端末間に伝送される情報を処理するために設けられている。適切なキーおよび他のパラメータは、セキュリティモジュールＳＭ１およびＳＭ２のメモリに配置される。公開キーは、前もってこのために予約された、たとえば特別な公開キーサーバからロードされることができる。

【００３７】

加えて、図２に示されるセキュリティシステムは、サービスプロバイダのサーバ８を含む。第１セキュリティモジュールは、本実施の形態では電話網である電気通信網を介してサービスプロバイダのサーバ８に接続されている。したがって、サービス利用者の端末によって実行された機能は、サーバに更新および保管することができる。また、サービスプロバイダの端末ＳＰおよびサーバ８は物理的に同じものであってもよい。

【００３８】

図３は、本発明に係る好適な移動局の概略図である。図３に示す移動局は、キーパッド９と、ディスプレイ１０と、無線装置１１と、電源１２と、および、ここで言及されない当然必要な他の構成要素とを含む。上述のように、必要なときに、セキュリティモジュールを通してなされる電子データ転送を暗号化し、暗号化された情報を解読し、電子署名を生成するための暗号化手段２と、電子データ転送を可能にするために移動局ＭＳおよび／または外部デバイスＳＰにセキュリティモジュールを接続するための第１接続インターフェースＩＦ１とを有するセキュリティモジュールＳＭは、電源１２に統合される。

【００３９】

セキュリティモジュールＳＭは、電気通信網および／または移動局のローカルインターフェース１３を介して移動局によって伝送される情報を処理するために設けられることが好ましい。したがって、たとえば、セキュリティモジュールがたとえばブルートゥースの技術を使用して移動局に最初の接続を確立し、同じ技術を使用してサービスプロバイダの端末ＳＰにさらに接続を確立するといった方法で、セキュリティモジュールはまた、移動局のデータ転送性質を利用できる。

【００４０】

図２を参照して、セキュリティシステム、セキュリティモジュール、および移動局の使用の好適な実施の形態が、以下に説明される。ユーザは、彼の預金口座から彼の電子マネー装置、すなわち移動局に、電子マネーをロードしたい。ユーザが移動局でたとえば銀行モードをスタートすると、セキュリティモジュールが作動し、その環境でブルートゥースの技術をサポートする他の装置と交信を始める。これは、ブルートゥースの解説に述べられる方法で実現できる。一旦、セキュリティモジュールＳＭ１がユーザの移動局ＭＳに接続され、そのキャッシュカードあるいはスマートカード構成要素ＳＣがオンラインバンキング端末ＳＰを検出すると、キャッシュカードあるいはスマートカード構成要素ＳＣは、自身の公開キーを送り、銀行の公開キーを受け取ることによって、銀行の端末との安全な接続を初期設定する。したがって、ユーザのセキュリティモジュールＳＭ１、およびオンラインバンキング端末のセキュリティモジュールＳＭ２は、メッセージを交換するときに、暗号化を使用できる。移動局ＭＳのキーパッド９、およびデ

ィスプレイ１０を使用することによって、ユーザはロードする金額を与え、その金額の情報が暗号化された形式でバンキング端末ＳＰに送信される。この後に、バンキング端末は、ユーザの電子署名を渡すことをユーザに求める。ここで、電子署名は、ユーザが自身のセキュリティモジュールＳＭ１を通して渡す。

【００４１】

オンラインバンキング端末ＳＰは、お金のロードの操作を認めた後、セキュリティモジュールＳＭ１およびＳＭ２を介してユーザのスマートカードＳＣに指定された金額を送り、この処理に関して銀行のサーバ８を更新する。ここで述べられないとはいえ、適当な変更を加え、さまざまなサービスおよび売買操作に上記機能が適用可能であることは明白である。

【００４２】

本発明は、上記した実施の形態の実例に制限されず、請求項に規定される発明の思想の範囲内で多くの変更が可能である。

【図面の簡単な説明】

【図１】　本発明に係るセキュリティモジュールを示す図である。

【図２】　本発明に係る好適なセキュリティシステムを示す図である。

【図３】　本発明により提供される統合されたセキュリティモジュールを含む本発明に係る好適な移動局を示す図である。

【符号の説明】

１…接続手段、

２…暗号化手段、

３、１２…電源、

４…プロセッサ、

６…フレーム、

７…コネクタ、

９…キーパッド、

１０…ディスプレイ、

１１…無線装置、

１３…移動局のローカルインターフェース、

ＩＦ１…第１接続インターフェース、

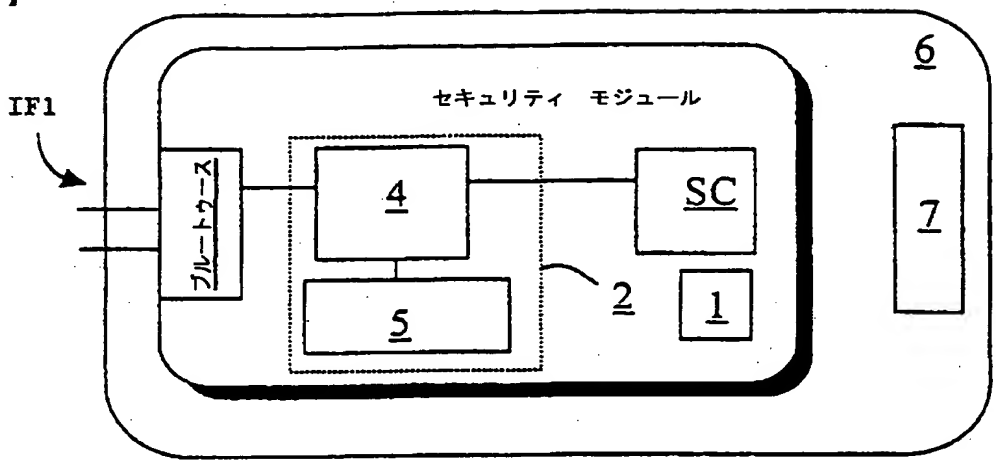
ＳＰ…サービスプロバイダの端末、

ＭＳ…サービス利用者の端末、

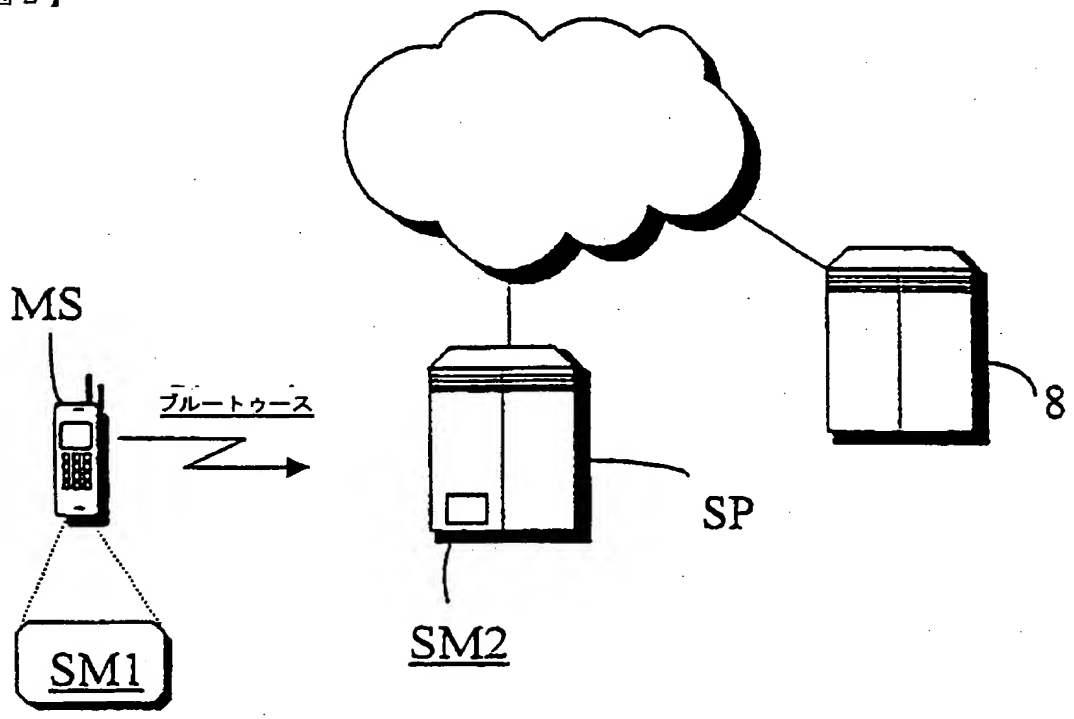
ＳＭ１、ＳＭ２…セキュリティモジュール、

ＳＣ…スマートカード構成要素。

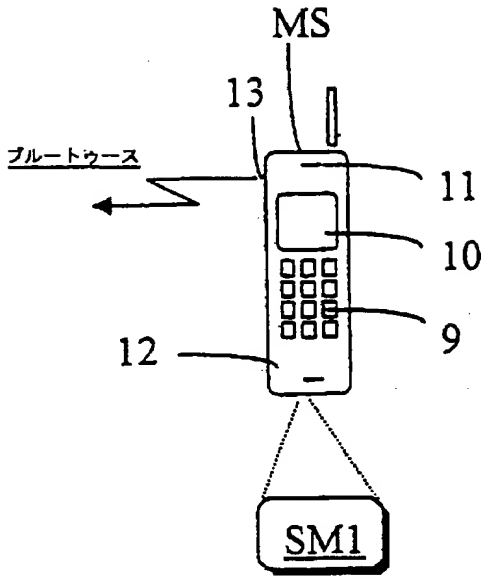
【図１】



【図２】



【図３】



【手続補正書】特許協力条約第３４条補正の翻訳文提出書

【提出日】平成１２年１０月１８日（２０００．１０．１８）

【手続補正１】

【補正対象書類名】明細書

【補正対象項目名】特許請求の範囲

【補正方法】変更

【補正内容】

【特許請求の範囲】

【請求項１】　移動局、レジ端末、オンラインバンキング端末、あるいはそれらの同等物のような端末装置（ＳＰ）にセキュリティモジュールを接続するための接続手段（１）を有する前記セキュリティモジュールであって、

前記セキュリティモジュールを通してなされる電子データ転送を暗号化し、暗号化された情報を解読し、電子署名を実現するための暗号化手段（２）と、

無線の電子データ転送を可能にするために外部デバイスに前記セキュリティモジュールを接続するための第１接続インターフェース（ＩＦ１）と、

電力を必要とする前記セキュリティモジュールの構成要素に電力を供給するための電源（３）と、

を有することを特徴とするセキュリティモジュール。

【請求項２】　前記暗号化手段は、

暗号化し、解読し、および電子署名を実現するプロセッサ（４）と、

前記プロセッサに必要とされるキーおよびパラメータを保管するために前記プロセッサに接続されるメモリ（５）と、

を有することを特徴とする請求項１に記載のセキュリティモジュール。

【請求項３】　前記セキュリティモジュールは、

前記セキュリティモジュールを通してスマートカード機能を実現するために設けられたスマートカード構成要素（ＳＣ）を有することを特徴とする請求項１または請求項２に記載のセキュリティモジュール。

【請求項４】　前記第１接続インターフェースは、ブルートゥースの技術使用して実現されることを特徴とする請求項１から請求項３のいずれか一項に記載

のセキュリティモジュール。

【請求項５】　前記セキュリティモジュールは、

移動局の電源の形状に一致するために適したフレームと、

実質的に前記移動局の電源の代わりに前記セキュリティモジュールを接続するため、および前記電源（３）から前記移動局に電力を供給するために、前記フレームに取り付けられるコネクタ（７）と、

を有することを特徴とする請求項１から請求項４のいずれか一項に記載のセキュリティモジュール。

【請求項６】　予め選択された通信リンクを通して電気的に相互に接続されるサービスプロバイダの端末（ＳＰ）と、サービス利用者の端末（ＭＳ）とを有するセキュリティシステムであって、

前記サービスプロバイダの端末に接続された第１セキュリティモジュール（ＳＭ１）と、

前記サービス利用者の端末に接続された第２セキュリティモジュール（ＳＭ２）とを有し、

前記各セキュリティモジュールは、端末間で通信リンクを通して伝送された情報を処理するために設けられ、

前記第１および第２セキュリティモジュールは、好ましくは、

前記セキュリティモジュールを通してなされた電子データ転送を暗号化し、暗号化された情報を解読し、電子署名を実現するための暗号化手段（２）と、

無線の電子データ転送のために端末に前記セキュリティモジュールを接続するための第１インターフェース（ＩＦ１）と、

電力を必要とするセキュリティモジュールの構成要素に電力を供給するための電源（３）とを有することを特徴とするセキュリティシステム。

【請求項７】　前記サービスプロバイダの端末（ＳＰ１）は、オンラインバンキング端末、レジ、自動販売機、あるいはそれらの同等物であることを特徴とする請求項６に記載のセキュリティシステム。

【請求項８】　サービス利用者の端末（ＳＰ２）は、移動局、ポータブルコンピュータ、あるいはそれらの同等物であることを特徴とする請求項６または請

求項７に記載のセキュリティシステム。

【請求項９】　サービスプロバイダのサーバ（８）を有し、

前記第１セキュリティモジュールは、サービス利用者の端末によって実行される機能を更新し、更新した前記機能を前記サーバに保管するために前記サービスプロバイダのサーバ（８）に前記電気通信網を通して接続されていることを特徴とする請求項６から請求項８のいずれか一項に記載のセキュリティシステム。

【請求項１０】　キーパッド（９）と、ディスプレイ（１０）と、無線装置（１１）と、電源（１２）とを有する移動局であって、

前記セキュリティモジュールを通してなされる電子データ転送を暗号化し、暗号化された情報を解読し、電子署名を実現するための暗号化手段（２）と、無線の電子データ転送を可能とするために、前記移動局（ＭＳ）および／または外部デバイス（ＳＰ）に前記セキュリティモジュールを接続するための第１インターフェース（ＩＦ１）とを有し、前記電源と統合されるセキュリティモジュール（ＳＭ）

を有することを特徴とする移動局。

【請求項１１】　前記セキュリティモジュール（ＳＭ）は、電気通信網および／または移動局のローカルインターフェース（１３）を通して移動局によって伝送される情報を処理するために設けられたことを特徴とする請求項１０に記載の移動局。

【請求項１２】　セキュリティモジュール（ＳＭ）は、ブルートゥースの技術を使用することによって、移動局（ＭＳ）および／またはサービスプロバイダの端末（ＳＰ）と通信するために設けられていることを特徴とする請求項１０または請求項１１に記載に移動局。

【国際調査報告】

1

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI 99/00713

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: H04Q 7/32, H04L 9/00
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7: H04Q, H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5742756 A (BLAIR B. DILLAWAY ET AL), 21 April 1998 (21.04.98), see whole document	1-3
Y		4-5
A		6-12
	--	
Y	Ericsson Review, Volume 3, 1998, Jaap Haartsen, "Bluetooth-The universal radio interface for ad hoc, wireless connectivity" page 117, column 1, line 53 - column 2, line 44	4-5
A		1-3,6-12
	--	

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" erlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
18 January 2000	19 -01- 2000
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Benny Andersson/MN Telephone No. +46 8 782 25 00

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI 99/00713

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 9837661 A1 (U.S. ROBOTICS MOBILE COMMUNICATIONS CORP.), 27 August 1998 (27.08.98) -- --------	1-12

INTERNATIONAL SEARCH REPORT

Information on patent family members

02/12/99

International application No.
PCT/FI 99/00713

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5742756 A	21/04/98	NONE	
WO 9837661 A1	27/08/98	AU 6165398 A	09/09/98

フロントページの続き

(81)指定国 EP(AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OA(BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG), AP(GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), EA(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW